

Managing Efficiently Future Pandemics

THE JOURNAL 2022

Áine Carroll
The Future of Healthcare in the Wake of
COVID-19 - Time for a Paradigm Shift

Jodi Keller, Nancy Lehr, Melissa Rose et al.
Surge Operations Call Center: Managing
Capacity Through Innovation and Collaboration

Giuseppe Tortora, Davide Caramella
Autonomous Delivery of Medical Material
Through Drones in a Future Pandemic

Hannah Jackson, Pooja Arora
The Challenges of Being a Locum GP Post
COVID-19

Amit Vaidya
Pharmaceutical Development Trends & Their
Impact on Healthcare Policy Planning & Delivery

Rahul Varshneya
Data Management Challenges in Healthcare
That Need to be Addressed to Improve Efficiency



Data Management Challenges in Healthcare That Need to be Addressed to Improve Efficiency

Rahul Varshneya | President and Co-founder | Arkenea Inc (Digital Health) | USA

An overview of data management challenges that can help improve efficiency, compliance, data security and interoperability in healthcare.



Key Points

- Every industry is striving to control and harness the power of data and healthcare is no exception.
- The Health Insurance Portability and Accountability Act (HIPAA), the HIPAA Security Rule and the HIPAA Privacy Rule have established national standards for the protection of electronic health information.
- It is critical for healthcare systems to execute robust data security solutions to help guarantee compliance.
- To integrate interoperability within their system, healthcare organisations need to streamline the data management process and make sure patient information is stored in a crisp, simplified and easily retrievable manner.
- The Healthcare Information and Management Systems Society (HIMSS) defines six technical controls and six operational controls to ensure data protection.

Today, one of the rudimentary questions that the universal wave of digitisation seeks to answer is how to optimise the use of data in order to amplify operational performance and create greater value in the process of doing so,

According to the recent “Harnessing the power of data in Health” [report by Stanford Medicine](#), systematic data management will continue to benefit healthcare in more than one way.

While data management has been bringing about essential transformations in healthcare, like in the case of every other innovation, it does not come without its unique set of challenges.

Here are some of the most common healthcare data management challenges that need to be addressed to improve efficiency on the provider’s part:

Adhering to Compliance and Regulations

The Health Insurance Portability and Accountability Act (HIPAA) enacted in 1996, and the HIPAA Security Rule and the HIPAA Privacy Rule issued by the Department of Health and Human Services (HHS) thereafter, established national standards for

the protection of health information, and specific electronic health information in particular.

Failing to abide by these rules can cost healthcare organisations hefty monetary penalties, and even subject them to criminal charges at times.

As per latest statistical data available at hand, 2018 was a record-breaker in terms of the total penalty amounts paid. The Office for Civil Rights (OCR), a part of the HHS which facilitates compliance activities, received \$28,683,400 in financial penalties in 2018. The mean financial penalty was \$2,607,582.

Some of the most commonly occurring HIPAA violations today are:

- Lack of a proper risk analysis and management process within a healthcare organisation.
- Failing to safeguard PHI (Protected Health Information) on personal or portable devices.
- Downloading or trying to gain access to ePHI through unauthorised devices.
- Prying on healthcare records.



- Releasing information to an unauthorised individual.
- Improper disposal of PHI.

Effective and regular staff training is vital to avoid HIPAA violations. Train your staff to be careful with PHI, and share it only with those authorised to know. If you have a HIPAA-compliant software, there are [guidelines](#) for that too that must be followed.

It doesn't matter if violations are the result of substandard human behaviour, gossip, insider or outsider hacking, or a mere

such as identification proofs among other things. This data is that slice of the pie which attracts cyber threats.

"Shadow IT and ransomware are only a part of the various issues the healthcare industry is currently facing. This is exactly why data security is one of the topmost priorities of providers across the globe right now," says Sameer Jafri, President and COO of [Avive Solutions](#).

The healthcare industry is expected to spend around \$65 billion on cybersecurity between 2017 and 2021. Healthcare

Healthcare data security legislation and best practices require robust physical security and compliance measures to be incorporated by healthcare organisations

human error. It is critical for healthcare systems to execute robust data security solutions to help guarantee compliance.

Making Data Interoperable

In order for data to be most utilitarian to any industry, it needs to furnish consistent value and should be shared amongst people, organisations, and systems. This forms the very foundation of interoperability.

"Data interoperability in healthcare streamlines patients' records from different electronic healthcare systems, allows patients to have absolute control over what information can be shared to whom, and simultaneously facilitates both innovation as well as research," says Andrew Kaluza, CEO, [TraceTheBody.com](#).

However, being one of the persevering challenges of the healthcare industry, data interoperability is not only difficult to achieve on the technical front, it also requires a consolidated structure of functions, as well as organisations' willingness to share information. There are several issues that arise when healthcare organisations look to make their data management systems interoperable.

For one, the amount of data to be retrieved and managed in hospitals on a regular basis is abundant, which makes the need for proper electronic record-keeping a prerequisite. When it comes to individual practitioners or office-based physicians, there is an inefficiency in proper record-keeping.

To overcome this persistent challenge and smoothly integrate interoperability within their system, healthcare organisations need to streamline the data management process and make sure that patient information is stored in a crisp, simplified and easily retrievable manner. This can only be done by syncing technology with manpower.

Providing Optimal Data Security

The healthcare industry operates enormous data assets which include protected health information and confidential data

data security legislation and best practices require robust physical security and compliance measures to be incorporated by healthcare organisations.

To be able to focus on its core business, a healthcare organisation must secure health information. The Healthcare Information and Management Systems Society (HIMSS) defines six technical controls to minimise security risks in its Healthcare security + Compliance Guide:

- Anti-malware software
- Data loss prevention software
- Two-factor authentication software
- Patch management software
- Disc encryption software
- Logging and monitoring software

Technical measures alone cannot guarantee complete data protection. A healthcare organisation also needs to have operational controls in place. The HIMSS report reveals six such controls:

- A security and compliance oversight committee
- Formal security assessment processes
- A security incident response plan
- Ongoing user awareness and training
- An information classification system
- Security policies

Lastly, improving efficiency through data management is really all about adopting a strategic approach whereby the three aspects of compliance, interoperability and data security are effectively addressed.

It is also crucial to comprehend the role of governments' support via an encouraging yet comprehensive legislation infrastructure, which allows the industry to manage and utilise data in ways that will yield the most value for patients.

Conflict of Interest

None. ■